



Wat gebeurt er nu echt als je een bestand verwijdt van je computer

...En hoe verwijderde bestanden juridisch voordeel kunnen opleveren

Veel mensen gaan ervan uit dat als ze een bestand van een computer verwijderen, bijvoorbeeld een tekstdocument of foto, het definitief verdwijnt. Dat is maar ten dele waar, soms blijft een verwijderd bestand nog lange tijd geheel of gedeeltelijk bestaan.

In dit artikel leg ik uit wat er gebeurt wanneer je een bestand verwijdt en wanneer herstel nog mogelijk is. Ook bespreek ik hoe je met digitaal forensisch onderzoek kunt aantonen dat een bestand ooit heeft bestaan, ondanks dat het is verwijderd. En hoe zelfs compleet verwijderde en vernietigde bestanden kunnen dienen als onweerlegbaar digitaal bewijs in juridische context.

Verwijderen ≠ vernietigen

Wanneer je een bestand verwijdt, gebeurt er technisch gezien niet zo veel. Het wordt namelijk niet echt verwijderd maar verplaatst naar de Recycle Bin (prullenbak). Zowel de originele data, de locatie van het bestand en de bijbehorende metadata blijven bewaard. De gebruiker van de computer kan het verwijderde bestand zelf eenvoudig herstellen door het uit de prullenbak te halen.

Pas als de Recycle Bin wordt geleegd, verandert de situatie. Dan wordt namelijk ook de verwijzing naar het bestand in het zogenoemde bestandssysteem verwijderd. Denk bij een bestandssysteem aan een structuur of manier waarmee besturingssystemen zoals Windows, data opslaan en beheren op een opslagmedium zoals een harde schijf. Het bestandssysteem houdt onder meer bij waar folders en bestanden zich precies bevinden op de harde schijf.

Echter, het bestand zelf wordt nog steeds niet permanent gewist. Het enige dat er gebeurt is dat de opslagruimte die het bestand inneemt op de harde schijf wordt gemarkeerd als free space. Dit betekent dat de opslagruimte beschikbaar wordt gesteld aan het besturingssysteem voor andere data. Het bestand is nu onzichtbaar geworden voor de gebruiker. Maar tot het moment dat de data daadwerkelijk wordt hergebruikt door andere bestanden, blijft het verwijderde bestand fysiek nog bestaan.

Met digitaal forensisch onderzoek bestaat afhankelijk van het type harde schijf, een relatief hoge kans op geheel of gedeeltelijk herstel van de verwijderde bestanden. Zelfs als het al enige tijd geleden is dat de bestanden zijn verwijderd.

Traditionele mechanische harde schijven vs Solid State Drives

De situatie zoals hierboven beschreven is de situatie waarbij de data is opgeslagen op traditionele mechanische harde schijven. De afgelopen jaren zijn mechanische harde schijven echter grotendeels vervangen door Solid State Drives (SSD) ook wel flash geheugen genoemd. Deze hebben vele voordelen ten opzichte van mechanische harde schijven. Zo hebben ze geen mechanische onderdelen en zijn ze beduidend sneller. Verder zijn ze stiller, energiezuiniger en robuuster.

Bij mechanische harde schijven blijft verwijderde data vaak nog lang intact en is er geen noodzaak om verwijderde data direct te wissen. Verwijderde data kan eenvoudig worden overschreven op het moment dat de schijfruimte nodig is voor het opslaan van andere data.

Bij SSD opslagmedia is dat totaal anders. Data wordt ingelezen en weggeschreven via elektrische signalen in plaats van een mechanische leeskop zoals bij mechanische harde schijven. Consequentie is dat vóórdat nieuwe data kan worden opgeslagen op een SSD, de opslagruimte wel eerst moeten worden vrijgemaakt van oude data. Een SSD weet anders niet welke opslagruimte ongebruikt of beschikbaar is en dat zou het proces van lezen en schrijven dusdanig vertragen dat het opslagmedium zeer traag wordt.

TRIM en Garbage Collection

Van een SSD verwijderde data moet dus wel eerst fysiek verwijderd worden voordat er nieuwe data kan worden opgeslagen. Hiervoor bestaat een SSD specifiek commando, TRIM. Dit is het commando dat het besturingssysteem, bijvoorbeeld Windows naar de SSD stuurt nadat de gebruiker een bestand heeft verwijderd. Het verschaft instructies aan de SSD en vertelt dat bepaalde opslagruimte niet meer in gebruik is. De SSD markeert die opslagruimte vervolgens voor opruiming, vaak al direct of binnen enkele seconden. Opruiming van de verwijderde data zelf gebeurt vervolgens door een proces met de illustere naam Garbage Collection (GC) ook wel Garbage Collector genoemd. Dit is een proces dat op de achtergrond van de computer actief is en onder meer ongebruikte geheugencellen opschoont door de data fysiek te verwijderen.

TRIM en GC zorgen ervoor dat verwijderde data soms al binnen enkele seconden tot minuten fysiek onherstelbaar wordt verwijderd en vernietigd. Hierdoor is herstel vrijwel onmogelijk geworden. Voor een digitaal forensisch onderzoeker betekent dit dat er snel gehandeld moet worden.

Wat als verwijderde bestanden niet meer te herstellen zijn

Stel je voor dat de verwijderde data niet meer herstelbaar is. Bijvoorbeeld doordat de data was opgeslagen op een SSD opslagmedium en TRIM en de Garage Collector hun werk hebben gedaan. Dan is het nog steeds niet onmogelijk om de data alsnog geheel of gedeeltelijk te herstellen. Bijvoorbeeld:

1. **Via de server.** De meeste zakelijke IT omgevingen zijn zo ingericht dat gebruikersdata zoals bestanden niet alleen op de computer van de gebruiker zijn opgeslagen maar ook binnen een zogenoemd gebruikersprofiel. Dit profiel is in de regel opgeslagen op een centrale server in een datacentrum. Vanuit kostenoverwegingen zijn de in datacentra gebruikte opslagmedia meestal nog steeds mechanische opslagmedia. Deze bieden (veel) langer kans op herstel van verwijderde data.
2. **Via backups.** Iedere informatiegestuurde organisatie maakt backups, of zou dat moeten doen ;-). Via backups is het vaak mogelijk om lang terug te gaan in de tijd. Soms zelfs langer dan 12 maanden.
3. **Via het bestandssysteem.** Iedere computer beschikt over een bestandssysteem waarin bepaalde metadata wordt geregistreerd over folders en bestanden, inclusief het bestandssysteem zelf. Deze metadata houdt tevens bij waar bestanden zich precies bevinden en wanneer deze zijn gecreëerd, geopend, veranderd en verwijderd. Zelfs als de data fysiek is verwijderd en niet meer te herstellen is, betekent dat niet dat alle sporen verdwenen zijn. Onder bepaalde omstandigheden kan via het bestandssysteem alsnog onweerlegbaar worden aangetoond dat specifieke bestanden ooit hebben bestaan.

Juridisch belang van verwijderde bestanden

Niet zelden zijn verwijderde bestanden doorslaggevend bewijs in juridische geschillen, bijvoorbeeld bij:

1. **Arbeidsconflicten**, waarbij een medewerker vlak voor ontslag bedrijfskritische of gevoelige bestanden wist zoals lead- en klantbestanden of offertes. Digitaal forensisch onderzoek kan aantonen wanneer en door wie bepaalde bestanden zijn verwijderd. Dit is mogelijk cruciaal bij ontslag op staande voet of schadeclaims.
2. **AVG en datalekken**, waar een organisatie bewust e-mailcommunicatie of logbestanden heeft verwijderd naar aanleiding van een datalek of cyberincident. Forensisch ICT onderzoek kan aantonen dat bepaalde data is vernietigd of gemanipuleerd, hetgeen invloed kan hebben op een eventuele sanctie of de mate van opgelopen reputatieschade.
3. **Kwesties inzake intellectueel eigendom**, waarbij concepten, broncode of ontwerpen zijn verdwenen of gekopieerd. Het kunnen aantonen dat een bepaald bestand ooit op een systeem heeft bestaan kan essentieel digitaal bewijs zijn bij intellectueel eigendom gerelateerde geschillen. Bijvoorbeeld bij onverwacht vertrek van een medewerker en zelfs bedrijfsspionage.

4. **Aandeelhouders- en bestuursgeschillen**, waarbij bepaalde bestuursleden bestanden rond besluitvorming of onderhandelingen hebben verwijderd. Herstel van deze data kan het bestaan van deze bestanden aantonen. Dit kan essentieel zijn bij juridische geschillen over onbehoorlijk bestuur.
5. **Strafzaken zoals zedenzaken en cybercrime**, waarbij een verdachte afbeeldingen, chatberichten of documenten heeft verwijderd. Digitale sporen, logbestanden en zelfs gedeeltelijk herstelde fragmenten kunnen strafvervolgning alsnog doorslaggevend beïnvloeden.
6. **Contractuele geschillen**, waar partijen bestanden of communicatie hebben verwijderd die afspraken of informeel gedane toezeggingen bevatten. Met digitaal bewijsmateriaal kunnen deze bestanden of sporen daarvan zoals tijdstempels en andere metadata alsnog een belangrijke rol spelen binnen juridische content of rechtszaak.
7. **Contra-expertise onderzoeken**, als belangrijk digitaal bewijsmateriaal lijkt te ontbreken. Een contra-expertise digitaal forensisch onderzoek kan aantonen dat er tijdens het initiële onderzoek fouten zijn gemaakt. Denk hierbij aan een situatie waarbij de digitaal forensisch onderzoeker alleen de onderzoeksvragen heeft beantwoord die relevant zijn voor de opdrachtgever, in dit geval de verdachte. Het gevolg kan zijn dat bepaalde belangrijke verwijderde bestanden onopgemerkt zijn gebleven, terwijl er duidelijke aanwijzingen waren dat iemand meerdere folders en bestanden had gewist. Ooggetuigen verklaarden dit persoonlijk te hebben gezien, vlak voordat de laptop werd ingeleverd bij de IT-afdeling.
8. **Financiële fraudezaken**, waarbij e-mailberichten met facturen of boekhoudkundige gegevens zijn gewist voor of na bijvoorbeeld een compliance controle. Digitaal forensisch onderzoek aan het bestandssysteem of een forensisch e-mailonderzoek kan aantonen dat geprobeerd is bepaald bewijsmateriaal te vernietigen.

Wat maakt verwijderde bestanden eigenlijk juridisch waardevol

1. Tijdstempels in het bestandssysteem geven onweerlegbaar aan wanneer bepaalde bestanden precies zijn verwijderd. Deze tijdstempels zijn dusdanig nauwkeurig dat zelfs fracties van secondes worden geregistreerd.
2. Verwijderde bestanden bieden herstelmogelijkheden waardoor de feitelijke inhoud kan worden ontsloten.
3. Gebruikerscontext geeft inzicht in wie bepaalde bestanden heeft verwijderd.
4. Systeem- en logbestanden en audit trails kunnen de feitelijke uitvoering van het verwijderen onderbouwen en bevestigen.

Conclusie

Verwijderen betekent lang niet altijd vernietigen, hoewel de mogelijkheden tot volledig herstel van verwijderde data de afgelopen jaren complexer zijn geworden.

Het kunnen aantonen dat een bepaald bestand op enig moment heeft bestaan en het op een specifiek moment opzettelijk is verwijderd, blijft vaak nog steeds onweerlegbaar aantoonbaar. Het blijft daarmee sterk digitaal bewijsmateriaal dat kan worden gebruikt in juridische context.

Vanuit digitaal forensisch perspectief is een verwijderd bestand niet het einde maar het begin. Verwijderde bestanden zijn meestal nog niet helemaal verdwenen, tenzij je te lang wacht.

Heeft u vragen of vermoedt u dat binnen uw organisatie bestanden onrechtmatig zijn verwijderd? Neem vrijblijvend contact op voor een discreet adviesgesprek over digitaal forensisch onderzoek.



212 DIGITAAL FORENSISCH ONDERZOEK BV

NIEUWE GRACHT 3

2011 NB, HAARLEM

NEDERLAND

© 212 DIGITAAL FORENSISCH ONDERZOEK BV | +31(0)23 303 5399 | DIGITAALFORENSISCHONDERZOEK.NL | KVK # 95758992